Troubleshooting

This chapter provides troubleshooting procedures for basic problems with the access point. For the most up-to-date, detailed troubleshooting information, refer to the Cisco TAC website at the following URL (select **Top Issues** and then select **Wireless Technologies)**:

http://www.cisco.com/tac

Sections in this chapter include:

- Checking the Top Panel Indicators, page 22-2
- Checking Basic Settings, page 22-5
- Resetting to the Default Configuration, page 22-5
- Reloading the Access Point Image, page 22-8

Checking the Top Panel Indicators

If your access point is not communicating, check the three LED indicators on the top panel to quickly assess the unit's status. Figure 22-1 shows the indicators on the 1200 series access point. Figure 22-2 shows the indicators on the 1100 series access point. Figure 22-3 and Figure 22-4 show the indicators on the 350 series access point.

Figure 22-1 Indicators on the 1200 Series Access Point

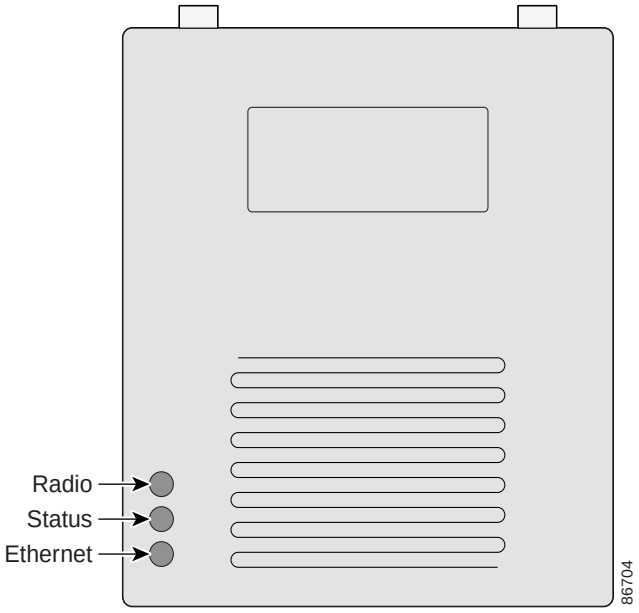


Figure 22-2 Indicators on the 1100 Series Access Point

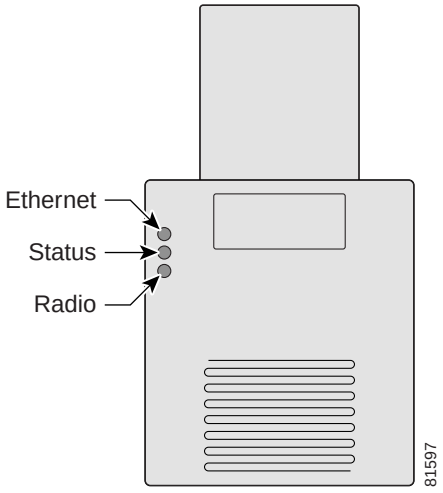


Figure 22-3 Indicators on the 350 Series Access Point (Plastic Case)

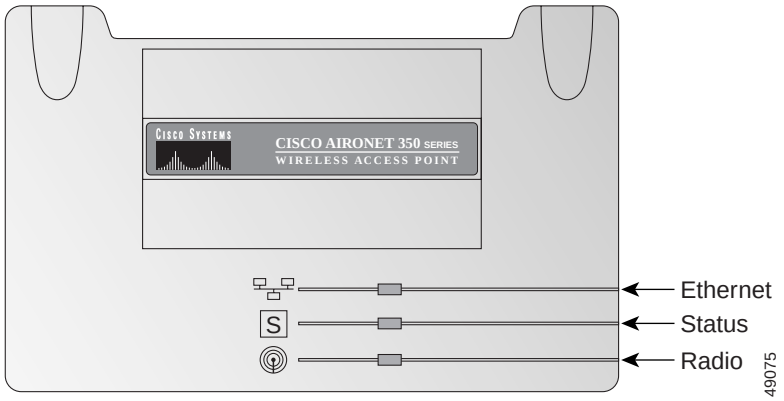
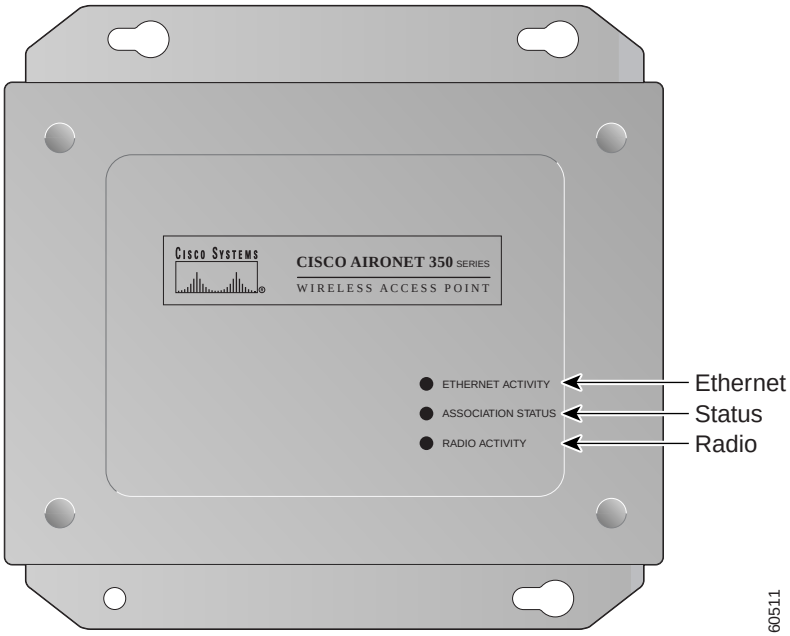


Figure 22-4 Indicators on the 350 Series Access Point (Metal Case)



The indicator signals have the following meanings (for additional details refer to Table 22-1):

- The Ethernet indicator signals traffic on the wired LAN. This indicator is normally green when an Ethernet cable is connected, and blinks green when a packet is received or transmitted over the Ethernet infrastructure. The indicator is off when the Ethernet cable is not connected.
- The status indicator signals operational status. Steady green indicates that the access point is associated with at least one wireless client. Blinking green indicates that the access point is operating normally but is not associated with any wireless devices.
- The radio indicator blinks green to indicate radio traffic activity. The light is normally off, but it blinks whenever a packet is received or transmitted over the access point's radio.

Table 22-1 Top Panel Indicator Signals

Message type	Ethernet indicator	Status indicator	Radio indicator	Meaning
Boot loader status	Green	–	Green	DRAM memory test.
	–	Amber	Red	Board initialization test.
	–	Blinking green	Blinking green	Flash memory test.
	Amber	Green	–	Ethernet initialization test.
	Green	Green	Green	Starting Cisco IOS software.
Association status	–	Green	–	At least one wireless client device is associated with the unit.
	–	Blinking green	–	No client devices are associated; check the unit's SSID and WEP settings.
Operating status	–	Green	Blinking green	Transmitting/receiving radio packets.
	Green	–	–	Ethernet link is operational.
	Blinking green	–	–	Transmitting/receiving Ethernet packets.
Boot Loader Errors	Red	–	Red	DRAM memory test failure.
	–	Red	Red	File system failure.
	Red	Red	–	Ethernet failure during image recovery.
	Amber	Green	Amber	Boot environment error.
	Red	Green	Red	No Cisco IOS image file.
	Amber	Amber	Amber	Boot failure.
Operation Errors	–	Green	Blinking amber	Maximum retries or buffer full occurred on the radio.
	Blinking amber	–	–	Transmit/receive Ethernet errors.
	–	Blinking amber	–	General warning.
Configuration Reset	–	Amber	–	Resetting the configuration options to factory defaults.
Failures	Red	Red	Red	Firmware failure; try disconnecting and reconnecting unit power.
	Blinking red	–	–	Hardware failure. The access point must be replaced.
Firmware Upgrade	–	Red	–	Loading new firmware image.

Checking Basic Settings

Mismatched basic settings are the most common causes of lost connectivity with wireless clients. If the access point does not communicate with client devices, check the following areas.

SSID

Wireless clients attempting to associate with the access point must use the same SSID as the access point. If a client device's SSID does not match the SSID of an access point in radio range, the client device will not associate. The access point default SSID is *tsunami*.

WEP Keys

The WEP key you use to transmit data must be set up exactly the same on your access point and any wireless devices with which it associates. For example, if you set WEP Key 3 on your client adapter to 0987654321 and select it as the transmit key, you must set WEP Key 3 on the access point to exactly the same value. The access point does not need to use Key 3 as its transmit key, however.

Refer to Chapter 9, "Configuring Cipher Suites and WEP," for instructions on setting the access point's WEP keys.

Security Settings

Wireless clients attempting to authenticate with your access point must support the same security options configured in the access point, such as EAP or LEAP, MAC address authentication, Message Integrity Check (MIC), WEP key hashing, and 802.1X protocol versions.

If a wireless client is unable to authenticate with your access point, contact the system administrator for proper security settings in the client adapter and for the client adapter driver and firmware versions that are compatible with the access point settings.

Note The access point MAC address that appears on the Status page in the Aironet Client Utility (ACU) is the MAC address for the access point radio. The MAC address for the access point Ethernet port is printed on the label on the back of the access point.

Resetting to the Default Configuration

If you forget the password that allows you to configure the access point, you may need to completely reset the configuration. On 1100 and 1200 series access points, you can use the MODE button on the access point or the web-browser interface. On 350 series access points, you can use the web-browser or CLI interfaces.

Note The following steps reset *all* configuration settings to factory defaults, including passwords, WEP keys, the IP address, and the SSID. The default username and password are both **Cisco**, which is case-sensitive.

Using the MODE Button

Follow these steps to delete the current configuration and return all access point settings to the factory defaults using the MODE button.

Note You cannot use the mode button to reset the configuration to defaults on 350 series access points. To reset the configuration on 350 series access points, follow the instructions in the "Using the Web Browser Interface" section on page 22-6, or in the "Using the CLI" section on page 22-7.

Step 1 Disconnect power (the power jack for external power or the Ethernet cable for in-line power) from the access point.

Step 2 Press and hold the **MODE** button while you reconnect power to the access point.

Step 3 Hold the **MODE** button until the Status LED turns amber (approximately 1 to 2 seconds), and release the button.

Step 4 After the access point reboots, you must reconfigure the access point by using the Web-browser interface or the CLI.

Note The access point is configured with the factory default values including the IP address (set to receive an IP address using DHCP). The default username and password are **Cisco**, which is case-sensitive.

Using the Web Browser Interface

Follow these steps to delete the current configuration and return all access point settings to the factory defaults using the web browser interface:

Step 1 Open your Internet browser. You must use Microsoft Internet Explorer (version 5.x or later) or Netscape Navigator (version 4.x).

Step 2 Enter the access point's IP address in the browser address line and press **Enter**. An Enter Network Password screen appears.

Step 3 Enter your username in the User Name field.

Step 4 Enter the access point password in the Password field and press **Enter**. The Summary Status page appears.

Step 5 Click **System Software** and the System Software screen appears.

Step 6 Click **System Configuration** and the System Configuration screen appears.

Step 7 Click the **Reset to Defaults** button.

Note If the access point is configured with a static IP address, the IP address does not change.

Step 8 After the access point reboots, you must reconfigure the access point by using the Web-browser interface or the CLI. The default username and password are **Cisco**, which is case-sensitive.

Using the CLI

Follow the steps below to delete the current configuration and return all access point settings to the factory defaults using the CLI.

Step 1 Open the CLI using a Telnet session or a connection to the access point console port.

Step 2 Reboot the access point by removing power and reapplying power.

Step 3 Let the access point boot until the command prompt appears and the access point begins to inflate the image. When you see these lines on the CLI, press **Esc**:

```
Loading "flash:/c350-k9w7-mx.v122_13_ja.20031010/c350-k9w7-mx.v122_13_ja.20031010"
...################################################################################
################################################################################
################################################################################
####################
```

Step 4 At the ap: prompt, enter the **flash_init** command to initialize the Flash.

```
ap: flash_init
Initializing Flash...
flashfs[0]: 142 files, 6 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 7612416
flashfs[0]: Bytes used: 3407360
flashfs[0]: Bytes available: 4205056
flashfs[0]: flashfs fsck took 0 seconds.
...done initializing Flash.
```

Step 5 Use the **dir flash:** command to display the contents of Flash and find the config.txt configuration file.

```
ap: dir flash:
Directory of flash:/
3 .rwx 223 <date> env_vars
4 .rwx 2190 <date> config.txt
5 .rwx 27 <date> private.config
150 drwx 320 <date> c350.k9w7.mx.122.13.JA
4207616 bytes available (3404800 bytes used)
```

Step 6 Use the **rename** command to change the name of the config.txt file to config.old.

```
ap: rename flash:config.txt flash:config.old
```

Step 7 Use the **reset** command to reboot the access point.

```
ap: reset
Are you sure you want to reset the system (y/n)?y
System resetting..Xmodem file system is available.
flashfs[0]: 142 files, 6 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 7612416
flashfs[0]: Bytes used: 3407360
flashfs[0]: Bytes available: 4205056
flashfs[0]: flashfs fsck took 0 seconds.
Reading cookie from flash parameter block...done.
```

```
Base ethernet MAC Address: 00:40:96:41:e4:df
Loading "flash:/c350.k9w7.mx.122.13.JA/c350.k9w7.mx.122.13.JA"...######## . . .
```

Note The access point is configured with factory default values, including the IP address (set to receive an IP address using DHCP) and the default username and password (**Cisco**).

Step 8 When IOS software is loaded, you can use the **del** privileged EXEC command to delete the config.old file from Flash.

```
ap# del flash:config.old
Delete filename [config.old]
Delete flash:config.old [confirm]
ap#
```

Reloading the Access Point Image

If your access point has a firmware failure, you must reload the complete access point image file using the Web browser interface or on 1100 and 1200 series access points, by pressing and holding the MODE button for around 30 seconds. You can use the browser interface if the access point firmware is still fully operational and you want to upgrade the firmware image. However, you can use the MODE button when the access point has a corrupt firmware image. On 350 series access points, you cannot use the MODE button to reload the image file, but you can use the CLI through a Telnet or console port connection.

Using the MODE button

You can use the MODE button on 1100 and 1200 series access points to reload the access point image file from an active Trivial File Transfer Protocol (TFTP) server on your network or on a PC connected to the access point Ethernet port.

Note You cannot use the mode button to reload the image file on 350 series access points. To reload the image file on 350 series access points, follow the instructions in the "Using the CLI" section on page 22-10.

Note If your access point experiences a firmware failure or a corrupt firmware image, indicated by three red LED indicators, you must reload the image from a connected TFTP server.

Note This process resets *all* configuration settings to factory defaults, including passwords, WEP keys, the access point IP address, and SSIDs.

Follow these steps to reload the access point image file:

Step 1 The PC you intend to use must be configured with a static IP address in the range of 10.0.0.2 to 10.0.0.30.

Step 2 Make sure that the PC contains the access point image file (such as *c1100-k9w7-tar.122-15.JA.tar* for an 1100 series access point or *c1200-k9w7-tar.122-15.JA.tar* for a 1200 series access point) in the TFTP server folder and that the TFTP server is activated. For additional information, refer to the "Obtaining the Access Point Image File" and "Obtaining TFTP Server Software" sections.

Step 3 Rename the access point image file in the TFTP server folder to **c1100-k9w7-tar.default** for an 1100 series access point or **c1200-k9w7-tar.default** for a 1200 series access point.

Step 4 Connect the PC to the access point using a Category 5 (CAT5) Ethernet cable.

Step 5 Disconnect power (the power jack for external power or the Ethernet cable for in-line power) from the access point.

Step 6 Press and hold the **MODE** button while you reconnect power to the access point.

Step 7 Hold the **MODE** button until the status LED turns red (approximately 20 to 30 seconds), and release the MODE button.

Step 8 Wait until the access point reboots as indicated by all LEDs turning green followed by the Status LED blinking green.

Step 9 After the access point reboots, you must reconfigure the access point by using the Web-browser interface or the CLI.

Using the Web Browser Interface

You can also use the Web browser interface to reload the access point image file. The Web broswer interface supports loading the image file using HTTP or TFTP interfaces.

Note Your access point configuration does not change when you use the browser to reload the image file.

Browser HTTP Interface

The HTTP interface enables you to browse to the access point image file on your PC and download the image to the access point. Follow the instructions below to use the HTTP interface:

Step 1 Open your Internet browser. You must use Microsoft Internet Explorer (version 5.x or later) or Netscape Navigator (version 4.x).

Step 2 Enter the access point's IP address in the browser address line and press **Enter**. An Enter Network Password screen appears.

Step 3 Enter your username in the User Name field.

Step 4 Enter the access point password in the Password field and press **Enter**. The Summary Status page appears.

Step 5 Click the **System Software** tab and then click **Software Upgrade**. The HTTP Upgrade screen appears.

Step 6 Click **Browse** to find the image file on your PC.

Step 7 Click **Upload**.

For additional information, click the **Help** icon on the Software Upgrade screen.

Browser TFTP Interface

The TFTP interface allows you to use a TFTP server on a network device to load the access point image file. Follow the instructions below to use a TFTP server:

Step 1 Open your Internet browser. You must use Microsoft Internet Explorer (version 5.x or later) or Netscape Navigator (version 4.x).

Step 2 Enter the access point's IP address in the browser address line and press **Enter**. An Enter Network Password screen appears.

Step 3 Enter your username in the User Name field.

Step 4 Enter the access point password in the Password field and press **Enter**. The Summary Status page appears.

Step 5 Click the **System Software** tab and then click **Software Upgrade**. The HTTP Upgrade screen appears.

Step 6 Click the **TFTP Upgrade** tab.

Step 7 Enter the IP address for the TFTP server in the TFTP Server field.

Step 8 Enter the file name for the access point image file in the Upload New System Image Tar File field. If the file is located in a subdirectory of the TFTP server root directory, include the relative path of the TFTP server root directory with the filename. If the file is located in the TFTP root directory, enter only the filename.

Step 9 Click **Upload**.

For additional information click the **Help** icon on the Software Upgrade screen.

Using the CLI

Follow the steps below to reload the access point image using the CLI. When the access point begins to boot, you interrupt the boot process and use boot loader commands to load an image from a TFTP server to replace the image in the access point.

Note Your access point configuration is not changed when using the CLI to reload the image file.

Step 1 Open the CLI using a Telnet session or a connection to the access point console port.

Step 2 Reboot the access point by removing power and reapplying power.

Step 3 Let the access point boot until it begins to inflate the image. When you see these lines on the CLI, press **Esc**:

```
Loading "flash:/c350-k9w7-mx.v122_13_ja.20031010/c350-k9w7-mx.v122_13_ja.20031010"
...################################################################################
################################################################################
################################################################################
####################
```

Step 4 When the ap: command prompt appears, enter the **set** command to assign an IP address, subnet mask, and default gateway to the access point.

Note You must use upper-case characters when you enter the **IP-ADDR**, **NETMASK**, and **DEFAULT_ROUTER** options with the **set** command.

Your entries might look like this example:

```
ap: set IP_ADDR 192.168.133.160
ap: set NETMASK 255.255.255.0
ap: set DEFAULT_ROUTER 192.168.133.1
```

Step 5 Enter the **tftp_init** command to prepare the access point for TFTP.

```
ap: tftp_init
```

Step 6 Enter the **tar** command to load and inflate the new image from your TFTP server. The command must include this information:

- the **-xtract** option, which inflates the image when it is loaded
- the IP address of your TFTP server
- the directory on the TFTP server that contains the image
- the name of the image
- the destination for the image (the access point Flash)

Your entry might look like this example:

```
ap: tar -xtract tftp://192.168.130.222/images/c350-k9w7-tar.122-13.JA1 flash:
```

Step 7 When the display becomes full the CLI pauses and displays `--MORE--`. Press the spacebar to continue.

```
extracting info (229 bytes)
c350-k9w7-mx.122-13.JA1/ (directory) 0 (bytes)
c350-k9w7-mx.122-13.JA1/html/ (directory) 0 (bytes)
c350-k9w7-mx.122-13.JA1/html/level1/ (directory) 0 (bytes)
extracting c350-k9w7-mx.122-13.JA1/html/level1/appsui.js (558 bytes)
extracting c350-k9w7-mx.122-13.JA1/html/level1/back.htm (205 bytes)
extracting c350-k9w7-mx.122-13.JA1/html/level1/cookies.js (5027 bytes).
extracting c350-k9w7-mx.122-13.JA1/html/level1/forms.js (15704 bytes)...
extracting c350-k9w7-mx.122-13.JA1/html/level1/sitewide.js (14621 bytes)...
extracting c350-k9w7-mx.122-13.JA1/html/level1/config.js (2554 bytes)
extracting c350-k9w7-mx.122-13.JA1/html/level1/stylesheet.css (3215 bytes)
c350-k9w7-mx.122-13.JA1/html/level1/images/ (directory) 0 (bytes)
extracting c350-k9w7-mx.122-13.JA1/html/level1/images/ap_title_appname.gif (1422 bytes)
extracting c350-k9w7-mx.122-13.JA1/html/level1/images/apps_button_1st.gif (1171 bytes)
extracting c350-k9w7-mx.122-13.JA1/html/level1/images/apps_button_cbottom.gif (318 bytes)
extracting c350-k9w7-mx.122-13.JA1/html/level1/images/apps_button_current.gif (348 bytes)
extracting c350-k9w7-mx.122-13.JA1/html/level1/images/apps_button_last.gif (386 bytes)
extracting c350-k9w7-mx.122-13.JA1/html/level1/images/apps_button_last_filler.gif (327
bytes)
```

```
extracting c350-k9w7-mx.122-13.JA1/html/level1/images/apps_button_last_flat.gif (318
bytes)
extracting c350-k9w7-mx.122-13.JA1/html/level1/images/apps_button_nth.gif (1177 bytes)
extracting c350-k9w7-mx.122-13.JA1/html/level1/images/apps_leftnav_dkgreen.gif (869 bytes)
 -- MORE --
```

If you do not press the spacebar to continue, the process eventually times out and the access point stops inflating the image.

Step 8 Enter the **set BOOT** command to designate the new image as the image that the access point uses when it reboots. The access point creates a directory for the image that has the same name as the image, and you must include the directory in the command. Your entry might look like this example:

```
ap: set BOOT flash:/c350-k9w7-mx.122-13.JA1/c350-k9w7-mx.122-13.JA1
```

Step 9 Enter the **set** command to check your bootloader entries.

```
ap: set
BOOT=flash:/c350-k9w7-mx.122-13.JA1/c350-k9w7-mx.122-13.JA1
DEFAULT_ROUTER=192.168.133.1
IP_ADDR=192.168.133.160
NETMASK=255.255.255.0
```

Step 10 Enter the **boot** command to reboot the access point. When the access point reboots, it loads the new image.

```
ap: boot
```

Obtaining the Access Point Image File

You can obtain the access point image file from the Cisco.com software center by following these steps:

Step 1 Use your Internet browser to access the Cisco Software Center at the following URL:

http://www.cisco.com/public/sw-center/sw-wireless.shtml

Step 2 Find the access point firmware and utilities section and click on the link for the 350, 1100, or 1200 series access point.

Step 3 Double-click the latest firmware image file, such as *c1100-k9w7-tar.122-11.JA* for 1100 series access points or *c1200-k9w7-tar.122-11.JA* for 1200 series access points.

Step 4 Download the access point image file to a directory on your PC hard drive.

Obtaining TFTP Server Software

You can download TFTP server software from several websites. Cisco recommends the shareware TFTP utility available at this URL:

http://tftpd32.jounin.net

Follow the instructions on the website for installing and using the utility.